## ENCRYPTION KEY MANAGEMENT METHOD OF SHARED ENCRYPTION INFORMATION

Publication number: JP2004048479 (A)

Publication date: 2004-02-12

Inventor(s): MIYAKE MASARU; NAKAO KOJI +

Applicant(s): KDDI CORP +

Classification:

- international: G06F15/00; G06F21/20; H04L9/08; G06F15/00; G06F21/20; H04L9/08; (IPC1-

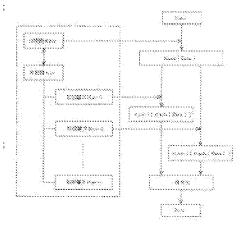
7): G06F15/00; H04L9/08

- European:

**Application number:** JP20020204495 20020712 **Priority number(s):** JP20020204495 20020712

## Abstract of JP 2004048479 (A)

PROBLEM TO BE SOLVED: To provide an encryption key management method of shared encryption information capable of exchanging an encryption key easily and safely with high confidentiality of the shared encryption information.; SOLUTION: A secret key Kpri of a public key encryption is divided into two or more secret key pieces Kpri-1, Kpri-2,..., Kpri-n by using an algorithm of a threshold encryption system, imperfectly decrypted information Kpri-1[Kpub [Data]], Kpri-2 [Kpub [Data]] is generated by decrypting information Kpub[Data] encrypted by a public key Kpub at different position, respectively, by using the number defined as a threshold of secret key pieces Kpri-1, Kpri-2, and information Data is reproduced by collecting the decrypted information Kpri-1[Kpub [Data]], Kpri-2 [Kpub [Data]] to a position to which an access is allowed.; COPYRIGHT: (C)2004,JPO



Data supplied from the *espacenet* database — Worldwide